UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/553,984 | 10/20/2005 | Hideo Sato | 273868US6PCT | 1022 |

22850 7590 09/03/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER |
|---|
| KING, JOHN B |

| ART UNIT | PAPER NUMBER |
|---|---|
| 4148 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 09/03/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/553,984 | SATO, HIDEO | |
| | Examiner | Art Unit | |
| | JOHN B. KING | 4148 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *20 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 October 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20 October 2005, 7 November 2006, 27 June 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. The instant application having Application No. 10553984 filed on October 20, 2005 is presented for examination by the examiner.

### *Oath/Declaration*

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

### *Priority*

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on February 24, 2004 (JAPAN 2004-48457).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

### *Drawings*

4. The applicant's drawings submitted are acceptable for examination purposes.

### *Specification*

**5.** The disclosure is objected to because of the following informalities: **On page 6 of the written description the diffusion plate is referred to as reference number 25, but the drawings label the diffusion plate as reference number 26. Also, the**

**shielding unit is referred to as reference number 26 in the written description, but labeled as reference number 25 in the drawings.**

Appropriate correction is required.

**6.** The disclosure is objected to because of the following informalities: **The term "humming distance" is used throughout the written description. The examiner believes that this is a common misspelling of "hamming distance." If this is not the case, the exact definition of the term "humming distance" should be defined in the specification. One example of "humming distance" can be found on page 11 of the written description.**

Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims **2-4, and 7-9** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. As per **claim 2, 3, and 8** the limitation of creating a "combination of correlation values between the signal and the evaluation patterns" renders this claim as vague and indefinite. It is unclear as to what the "evaluation patterns" are. Furthermore, it is also

unclear as to what a “combination of correlation values between the signal and the evaluation patterns” means.

10. As per **claim 7** the limitation of creating a "combination of correlation values between the signal and a plurality of different evaluation patterns" renders this claim as vague and indefinite. It is unclear as to what the "evaluation patterns" are. Furthermore, it is also unclear as to what a “combination of correlation values between the signal and a plurality of different evaluation patterns” means.

11. **Claim 4** recites the limitation "the uniform imaging target" in line 6. There is insufficient antecedent basis for this limitation in the claim. It is not clear to the examiner whether the applicant refers to the “prescribed imaging target” or some other imaging target. It appears to the examiner that applicant is referring to "the prescribed imaging target."

12. **Claim 9** recites the limitation "the solid imaging element" in lines 3-4. There is insufficient antecedent basis for this limitation in the claim.

### *Claim Rejections - 35 USC § 102*

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14. **Claims 1, 4, 6, and 9** are rejected under 35 U.S.C. 102(b) as being anticipated by Bjorn (US Patent No. 6035398), published March 7, 2000.

As per **claim 1**, Bjorn discloses an encryption device for encrypting information on a confidential target, comprising: creation means for creating a unique parameter [key] of an element group based on a signal output [biometric data] from the element group internally having a plurality of elements as a unit (figures 3-9 and col. 1 lines 40-42 and col. 2 lines 4-22 and col. 6 lines 4-30, Bjorn teaches using biometric data to generate a cryptographic key. In figure 9 and its description in col. 6 lines 4-30, Bjorn teaches that the element group (fingerprint) has a plurality of elements.); and encryption means for encrypting [using] the information by using the unique parameter [key] created by the creation means (col. 4 lines 38-46, Bjorn teaches using the cryptographic key to encrypt a document).

As per **claim 4**, Bjorn discloses the encryption device according to claim 1 [See rejection to claim 1 above], comprising solid imaging element [feature extraction unit] for imaging a prescribed imaging target [fingerprint] (col. 3 lines 25-35, Bjorn teaches extracting and saving a user's fingerprint), wherein the creation means creates the unique parameter [key] of the solid imaging element based on a signal output from the solid imaging element as a result of imaging the uniform imaging target [fingerprint] (col. 4 lines 5-37, Bjorn teaches extracting one or more features from a fingerprint and creating a template which is then used to create a cryptographic key).

As per **claim 6,** Bjorn discloses an encryption method for encrypting information on a confidential target, comprising: a first step of creating a unique parameter [key] of

an element group based on a signal output [biometric data / fingerprint] from the element group internally having a plurality of elements as a unit (figure 9 and col. 6 lines 4-30, Bjorn discloses that a fingerprint is comprised of a plurality of elements); and a second step of encrypting the information by using the unique parameter [key] created (figures 3-9 and col. 1 lines 40-42 and col. 2 lines 4-22 and col. 4 lines 38-46, Bjorn teaches extracting a fingerprint by using a sensor and then generating a cryptographic key from the fingerprint data. In col. 4 lines 38-46, Bjorn also teaches using the key to encrypt or sign documents).

As per **claim 9**, Bjorn discloses the encryption method according to claim 6 [See rejection to claim 6 above], wherein the first step creates the unique parameter [key] of the solid imaging element [feature extraction unit] based on a signal output [biometric data / fingerprint] from the solid imaging element as a result of imaging a uniform imaging target [finger] (col. 4 lines 5-37, Bjorn teaches extracting one or more features from a fingerprint and creating a template which is then used to create a cryptographic key).

### *Claim Rejections - 35 USC § 103*

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. **Claims 2 and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn in view of Shinzaki (US 2003/0005310 A1), published January 2, 2003.

As per **claim 2**, Bjorn discloses the encryption device according to claim 1 [See rejection to claim 1 above]. Bjorn teaches using biometric data (fingerprint) to generate a cryptographic key. However, Bjorn does not teach storing evaluation patterns or using correlations to generate the cryptographic key.

Shinzaki discloses the creation means comprising storage means for storing a plurality of different evaluation patterns [valid biometric data], and creates a combination of correlation values between the signal and the evaluation patterns being stored in the storage means, as the unique parameter (paragraph 69, Shinzaki teaches using a correlation between "valid biometric data" and "to-be-verified biometric data" to determine if a user is authorized). Shinzaki also teaches storing a key (paragraph 10, Shinzaki discloses storing a key in a storage medium so that the user does not have to remember the key).

Bjorn and Shinzaki are analogous art because they are from the same field of endeavor of using biometric data.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the encryption system which generates a key by using a user fingerprint as described by Bjorn and adding the feature of generating the key by using a correlation between the user fingerprint / biometric data as taught by Shinzaki because it would allow for more secure key generation as well as user authentication.

As per **claim 7**, Bjorn discloses the encryption method according to claim 6 [See rejection to claim 6 above]. Bjorn teaches using biometric data (fingerprint) to generate a cryptographic key.

However, Bjorn does not disclose using correlations to generate a key.

Shinzaki discloses creating correlation values between the signal and a plurality of different evaluation patterns [valid biometric data], as the unique parameter [key] (paragraph 69, Shinzaki discloses a using a correlation between "valid biometric data" and "to-be-verified biometric data" to determine if a user is authorized).

Bjorn and Shinzaki are analogous art because they are from the same field of endeavor of key generation.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the encryption system which generates a key by using a user's biometric data (fingerprint) as taught by Bjorn by adding the feature of using correlation values as taught by Shinzaki because it would increase the security of the keys that were generated. By doing this it will be extremely difficult for someone to illegally obtain the key.

17. **Claims 3 and 8** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn in view of Shinzaki and Lee et al (US 2002/0087325 A1) hereinafter referred to as Lee, published July 4, 2002.

As per **claim 3**, Bjorn in view of Shinzaki discloses the encryption device according to claim 2 [See rejection to claim 2 above], comprising communication means

for communicating with a prescribed communication party [certification authority] (col. 8 lines 30-40, Bjorn teaches communicating with a certification authority in order to transfer a fingerprint template to determine if a user is authorized or not.)

However, Bjorn in view of Shinzaki does not teach letting the communication party request what evaluation patterns to perform the correlation between.

Lee discloses the creation means selecting evaluation patterns [authentication types] requested by the communication party [user], from the evaluation patterns being stored in the storage means (paragraph 154, Lee teaches allowing the user to authenticate themselves by using a variety of different ways such as voice signature or ID and PIN. By doing this the user can choose what type of authentication type they want to use to verify that they are a valid user).

Bjorn in view of Shinzaki and Lee are analogous art because they are from the same field of endeavor of using biometric data to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the encryption system which generates a key using a user fingerprint, allows for communicating with a communication party along with correlations for user authentication as described by Bjorn in view of Shinzaki and adding the feature of allowing the user to choose the authentication means as taught by Lee because it would allow for greater flexibility in the way that the users can authenticate themselves.

As per **claim 8**, Bjorn in view of Shinzaki discloses the encryption method according to claim 7 [See rejection to claim 7 above]. Bjorn in view of Shinzaki teaches key generation by using a user's biometric data and user authentication by using a

correlation between the user's biometric data and a set of valid biometric data. Bjorn in view of Shinzaki also teaches communication with another communication party.

However, Bjorn in view of Shinzaki does not disclose allowing the communication party to request a set of parameters on which the correlation will be performed.

Lee discloses selecting evaluation patterns [authentication types] meeting to a request made from a prescribed communication party [user] (paragraph 154, Lee teaches allowing the user to authenticate themselves by using a variety of different ways such as voice signature or ID and PIN. By doing this the user can choose what type of authentication type they want to use to verify that they are a valid user.)

Bjorn, Lee and Shinzaki are analogous art because they are from the same field of endeavor of using biometric data to perform user authentication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of generating a key based upon a user's fingerprint, allowing communication and performing correlations to authenticate a user as taught by Bjorn in view of Shinzaki by adding the feature of allowing the user/communication party to choose the authentication method because it would increase the security of the keys that were generated and also increase the flexibility of the system by giving the user more authentication choices.

18. **Claims 5 and 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn in view of Buttiker (US 2002/0176583 A1), published November 28, 2002.

As per **claim 5**, Bjorn discloses the encryption device according to claim 1 [See rejection to claim 1 above], comprising a solid imaging element [feature extraction unit] for imaging a prescribed imaging target [fingerprint] (col. 3 lines 25-35, Bjorn teaches extracting and saving a user's fingerprint), wherein: the creation means comprises: parameter creation means for creating the unique parameter [key] of the solid imaging element based on a signal output from the solid imaging element as a result of imaging. the uniform imaging target [fingerprint] (col. 4 lines 5-37, Bjorn teaches extracting one or more features from a fingerprint and creating a template which is later used to create the cryptographic key); and body information creation means for creating body information unique to a body [fingerprint] based on a signal output from the solid imaging element [feature extraction unit] as a result of imaging a surface of the body [fingerprint] or an inside of the body (col. 3 lines 25-35 and col. 4 lines 5-37, Bjorn teaches collecting information about a person (fingerprint) from a feature extraction unit. The fingerprint is a result of scanning/imaging a person's finger). However, Bjorn does not teach encrypting the user's body information.

Buttiker teaches the encryption means to encrypt the body information [biometric data] created by the body information creation means [biometric input device] by using the unique parameter [private key] created by the parameter creation means (paragraph 32, Buttiker discloses using a private key to encrypt a user's biometric data).

Bjorn and Buttiker are analogous art because they are from the same field of endeavor of using biometric data and cryptographic keys.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the fingerprint scanning system as taught by Bjorn and adding the feature of encrypting the biometric data (fingerprint) as taught by Buttiker because it would allow for more secure transfer of a user's biometric data that may be used illegally if received by some third party.

As per **claim 10**, Bjorn discloses the encryption method according to claim 6 [See rejection to claim 6 above], wherein: the first step comprises: a parameter creation step of creating the unique parameter [key] of a solid imaging element based on a signal output from the solid imaging element [feature extraction unit] as a result of imaging a uniform imaging target [fingerprint] (col. 4 lines 5-37, Bjorn teaches extracting one or more features from a fingerprint and creating a template which is then used to create a cryptographic key); and a body information creation step of creating body information unique to the body [fingerprint] based on a signal output from the solid imaging element [feature extraction unit] as a result of imaging a surface of the body [fingerprint] or an inside of the body (col. 3 lines 25-35 and col. 4 lines 5-37, Bjorn teaches collecting information about a person (fingerprint) from a feature extraction unit. The fingerprint is a result of scanning/imaging a person's finger). However, Bjorn does not teach encrypting the user's body information.

Buttiker teaches encrypting the body information [biometric data] by using the unique parameter [private key] (paragraph 32, Buttiker discloses using a private key to encrypt a user's biometric data).

Bjorn and Buttiker are analogous art because they are from the same field of endeavor of using biometric data and cryptographic keys.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the fingerprint scanning system as taught by Bjorn and adding the feature of encrypting the biometric data (fingerprint) as taught by Buttiker because it would allow for more secure transfer of a user's biometric data that may be used illegally if received by some third party.

## ***Conclusion***

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN B. KING whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Thur. 7:30 AM - 5:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148

JBK